Attack or Defend?

Leveraging Information and Balancing Risk in Cyberspace

Colonel Dennis M. Murphy, U.S. Army, Retired

When this article was originally written, DOD policy and military regulations significantly restricted the use of the Internet for strategic communication purposes in favor of security. On 25 February 2010, DOD published a policy embracing a balanced approach in this regard, thus supporting the original thesis of this article. The author has updated the article accordingly to provide a deeper explanation of the policy decision and as a call to embrace its tenets.

UNITED STATES MILITARY history is replete with examples of preparing for the next war by studying the last (or current) one. Consequently, we often engage in warfare with doctrine and processes that lag behind current reality. The result can be a prolonged war effort at great cost to national treasure, both fiscal and human. The harried development and implementation of counterinsurgency doctrine, resulting in the so-called "surge" in the midst of the campaign in Iraq, is but one example.[1]

The Army's introspective consideration of future warfare in the late 1970s and early 1980s, however, is an exception. Using the 1973 Arab-Israeli War as a harbinger of warfare where precision weaponry and technological advances showed the importance of maneuver, the Army shifted from a doctrine of "Active Defense" to "Airland Battle." However, this was not universally accepted. In a 2006 Landpower essay, Brigadier General Huba Wass de Czege remininisced:

> In what developed into a healthy exchange, [young officers] saw defensive tactics as a "fall-back by ranks" approach that confused delay and defense, and would lead commanders to avoid decisive engagement . . . They saw it as reactive, surrendering the initiative and resulting in a risky method of defense.[2]

The official history of the 1991 Gulf War describes the shift to Airland Battle doctrine as a prescient decision that was the basis of that dramatic victory for the U.S. military.[3]

So what will the next war look like? No one has a flawless crystal ball to predict the future, but even a cursory consideration of potential future

Colonel Dennis M. Murphy, U.S. Army, Retired, is the director of the Information in Warfare Group at the U.S. Army War College. Professor Murphy teaches elective courses on information operations and strategic communication, and he conducts workshops focused on the information element of national power.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2010		**00-05-2010 to 00-06-2010**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Attack or Defend? Leveraging Information and Balancing Risk in Cyberspace	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **U.S. Army Combined Arms Center,Fort Leavenworth,KS,66027**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

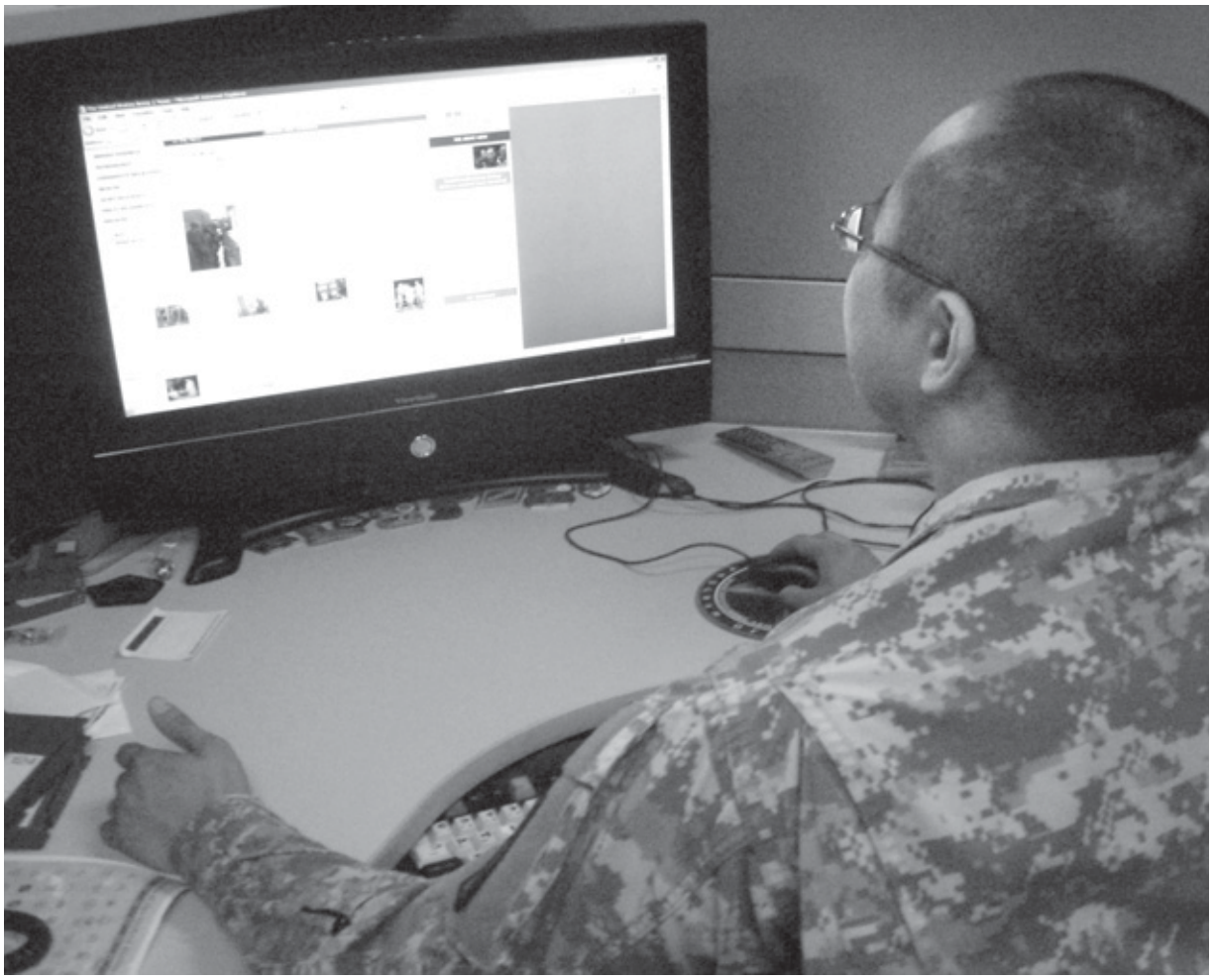
12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**9**	



U.S. Army photo by David Vergun

A Soldier enters cyberspace.

adversaries reveals the importance placed on information as a strategic asymmetric means to conduct warfare. The Chinese military has reportedly hacked into Pentagon military networks.[4] The Russian government allegedly conducted a major cyber attack on Estonian infrastructure.[5] Yet even while attacks on information systems are proving to be a threat, reliance on the Internet to fight the "war of ideas" is increasing. Consider the so-called "2nd Lebanon War" between Israel and Hezbollah in the summer of 2006. Hezbollah used information to affect perceptions as a means to achieve strategic victory, even going so far as to place billboards on the rubble of buildings in southern Lebanon that said "Made in the USA" (in English).[6]

The U.S. military certainly recognizes this threat, as the move to establish a U.S. Cyber Command demonstrates. However, until recently, doctrine was lagging. Past policies favored "active defense" over "maneuver" in cyberspace. And while a recent policy change points to a potentially significant shift in that equation, the question arises whether the military will embrace the organizational change necessary to balance the need to protect networks while going on the ideological offensive its adversaries have embraced.

In the end, leaders must weigh the risks involved to achieve a balance to compete in the information battlespace. Will they develop an "Airland Battle" equivalent for cyberspace, or will they wait until the next war to strike the balance at potentially great cost to our Nation?

Defining the Problem

Keeping up with the definition of cyberspace can be a full-time job. Since 2004, the U.S. government has presented four different "official"

definitions. The Department of Defense (DOD) currently defines cyberspace as—

> a global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[7]

Perhaps more important, cyberpower is "the ability to use cyberspace to create advantages and influence events in all the operational environments and across the instruments of power."[8] Thus, much like land, sea, and airpower, cyberpower is a weapon of war.

The DOD definition of cyberspace rightly recognizes the importance of the Internet as an enabler of that domain in today's information environment. The World Wide Web, as a subset of the Internet, is essentially ungoverned, providing obvious freedoms and cautions. The web gives the individual a voice—often an anonymous voice—and a potentially vast audience. One can easily establish, dismantle, and reestablish a website. This attribute makes them valuable to extremist movements. On the other hand, the same capability the web gives our adversaries is available to us, if we choose to embrace it. *The National Strategy for Combating Terrorism* notes that the Internet provides terrorists cyber safe havens to "communicate, recruit, train, rally support, proselytize, and spread their propaganda without risking personal contact." It also points out the opportunity the Internet offers to discredit that same propaganda.[9]

The impact of Internet technologies on national security and warfighting will not only increase in the future, but do so exponentially.[10] Consider the Internet as a significant means to conduct the "war of ideas." Web logs (blogs), YouTube, Google Earth, and Second Life are all "new media"—enabling technologies our adversaries use to gain asymmetric advantage by affecting perceptions, attitudes, behaviors, and ultimately beliefs. Social media sites such as Facebook and Twitter have exploded recently and are used for purposes well beyond the social interaction that this medium implies. The iPhone may look like a phone, but it has all the capabilities of a desktop computer (and more in many cases) in a device the size of your palm. There is no doubt that technology will continue to be faster, cheaper, and more capable. New media in this context quickly become "old" media. And so a more timeless definition sees new media as any capabilites that empower a broad range of actors (individuals through nation-states) to create and disseminate real-time or nearly real-time information that can affect a broad (regional or worldwide) audience. Although it was previously the exclusive purview of nation-states and large multi-national corporations, individuals can now wield information as a strategic means, a development of importance to policymakers and warfighters.

Future warfighting challenges must consider the almost certain use of the Internet by any potential adversary. Analysts should not gain a false sense of security based on limited Internet penetration in some of the most contentious parts of the world. While Africa has only a 6.8 percent Internet penetration based on population, the use of the Internet there grew 1,392 percent from 2000 to 2009. Dramatic growth rates are similarly occurring in Asia, the Middle East, and Latin America.[11]

Warfighters recognize the requirement to compete in cyberspace. Increasingly, senior leaders and units sponsor Facebook pages and "tweet" routinely. The U.S. Central Command engages dissident voices by participating in blogs that are critical of the war on terror, noting "with the proliferation of information today, if you're not speaking to this forum, you're not being heard by it."[12] The United States military also recognizes the importance of competing in the video medium, using YouTube to show ongoing images of U.S. operations in the current theaters of war.[13]

On the other hand, the U.S. military's significant dependence on the Internet for routine daily business and communication creates a vulnerability to cyber attack. There are plenty of people and organizations out there probing U.S. networks. While the U.S. repels most of those attacks, the failures provide a glimpse into their impact. China's People's

Warfighters recognize the requirement to compete in cyberspace.

Liberation Army attacked Pentagon computers in June 2007 apparently following numerous probes and caused the network to be taken down for more than a week.[14] The Chinese are transforming from a mechanized to an "informationized" force and have stated they intend to use information warfare "as a tool of war [or] as a way to achieve victory without war."[15] Retired General Barry McCaffrey indicates this is not an anomaly, but in fact may be the norm. He notes that all of our potential adversaries, as well as criminal elements, conduct daily reconnaissance of our electronic spectrum in areas critical to U.S. national security.[16] In fact, on average, U.S. government computer systems come under attack every eight seconds.[17]

The case of Estonia may be a precursor of what the United States could expect as it increases its reliance on the Internet for government and military business. Estonia uses some of the most advanced "e-government" processes in the world. Estonians bank, vote, and pay taxes online, and Estonia has embedded its national identification cards with electronic chips, making them very efficient and, as it turns out, very vulnerable. So it mattered when Russian hackers attacked in the spring of 2007.[18] In fact, some observers equated that cyber attack to an act of war in the Clausewitzian sense, with the intent to create mass social panic.[19]

It should not be surprising, then, that protecting the net has taken on great importance in the Department of Defense and that using that same net to get proactive, positive U.S. messages out is increasingly significant. A recent Department of Defense policy change has opened the aperture to enable opportunities to use the Internet to counter misinformation and tell the story of the American military. However, it remains to be seen whether organizational culture will embrace such an approach.

Defend: Protecting the Network

Great effort and resources go into protecting the Internet-capable systems of the Department of Defense and other governmental organizations. The Department of Homeland Security established a National Cybersecurity Center whose mission is to "coordinate and integrate information necessary to help secure U.S. cyber networks and systems and help foster collaboration among federal cyber groups."[20] The Department of Defense has codified the process to protect their networks in a concept called information assurance. Information assurance includes

> measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and nonrepudiation. This includes providing for restoration of information systems by incorporating protection, detection and reaction capabilities . . . IA [information assurance] requires a *defense-in-depth approach* [emphasis added].[21]

The Department of Defense conducts unclassified computer operations within a subset of the Internet known as the "NIPRnet" (originally the nonclassified Internet protocol router network). The NIPRnet isolates access to the greater Internet by using a limited number of portals or gateways. This methodology makes the required "defense in depth" manageable from a resource perspective in that it reduces the number of pathways to monitor for attacks. It allows access to the Internet to facilitate efficient business and command and control.[22] But firewalls and content filters that block entrance to specific external sites often limit access to the World Wide Web in order to promote work productivity, support bandwidth requirements, protect operations security, and prevent intrusion and compromise. In the recent past it appeared that this external access would become even more restrictive. Deputy Secretary of Defense Gordon England asked Congress for funds to build, for lack of a better term, a "DODnet" in July 2008. "Recent attacks from China on Department of Defense networks and systems increase the urgency to construct cyber systems that can't be penetrated."[23] The trend was toward increased security by locking down the system, an approach that was at odds with winning the war of ideas.

Attack: Getting the Message Out

Senior military leaders increasingly emphasize the importance of "strategic communication" to compete in the information environment. According to the Department of Defense, strategic communication is

> focused United States Government processes and efforts to understand and engage key audiences to create, strengthen, or

> preserve conditions favorable to advance national interests and objectives through the use of coordinated information, themes, plans, programs, and actions synchronized with other elements of national power.[24]

Thus, strategic communication is the integration of actions, images, and words to send a message to affect perceptions, attitudes, and behaviors.[25] Actions send the loudest messages, but images and words provide context and often have significant effects on their own. While strategic communication focuses on the cognitive dimension of the information environment, it relies on the physical environment to send its messages. Often that requires ready and rapid access to the Internet.

Leaders increasingly point to the importance of using new media means and the Internet to proactively fight in cyberspace. However, past anecdotal evidence reveals a struggle between defending the networks and using them to actively get out the message. U.S. operations in Iraq shown on YouTube were among the top 10 viewed for weeks after their posting, but the Army posted them only after senior generals overcame significant bureaucratic stonewalling.[26] Bandwidth considerations may have been an issue. Blogs are fast becoming the medium of choice not only for recreational, but for more serious military and political pursuits. Blogs provide a forum to tell the military's story, often by the most credible sources—the Soldiers, Sailors, Airmen, and Marines themselves—but risk-aversion often stymies the effort. Past military policies in Iraq have been restrictive and often discouraged blogging rather than encouraging it.[27] In May 2008, Army Lieutenant Matthew Gallagher's blog "Kaboom" was taken down by his leadership after he recounted an anonymous exchange between himself and his commander without seeking approval prior to posting it. Before its demise, the site received tens of thousands of page views about the day-to-day life of an Army platoon in the war zone.[28] MySpace and Facebook receive plenty of press about their transparency and the adverse effect of personal disclosure in the wrong hands. On the other hand, from a military perspective these social networking sites provide an opportunity to tell a credible and contextual story of military life. Both blogs and social networks, however, present operations

Photo by Prudence Siebert/Fort Leavenworth Lamp

Command and General Staff College students Majors Gary Belcher, Dexter Brookins, and Troy Newman work in the division main command post during the Digital Warfighter Exercise, Fort Leavenworth, KS, 14 February 2008.

security issues for commanders, rightly concerned about maintaining the secrecy of military operations, capabilities, and vulnerabilities.

Many senior military leaders acknowledge the importance of these new media tools as contemporary military capabilities and encourage participation in the dialogue that they facilitate. Examples from the recent past point to a risk averse climate at high levels that in turn works against capitalizing on the network's potential.[29] For example, in March 2008, the Army's Combined Arms Center (CAC) at Fort Leavenworth, Kansas, submitted a memorandum requesting an "exception to policy" to allow their officers to engage in blogging in the public domain.[30] CAC is commanded by a three-star general who had to go to his four-star command for that authority. What's more, CAC is responsible for training and educating Army leaders in the use of these capabilities.

The Department of Defense also restricted the authority to conduct interactive Internet activities to the four-star level and only allowed public affairs officers to engage in interactive Internet activities with journalists.[31] These policies not only appled to the NIPRnet but also restricted home use of the Internet.

What appears to be a significant breakthrough, however, occurred in February 2010 with the publication of a DOD memorandum entitled "Responsible and Effective Use of Internet-based Capabilites." This broad policy significantly softens the previous restrictions by explicitly directing NIPRnet access to a wide variety of publicly available collaborative tools and discussion forums. (The policy specifically cites YouTube, Facebook, and Twitter among others). On the other hand, commanders at all levels are directed to continue to defend against malicious activities and take action to safeguard missions.[32]

This recent policy seemingly makes sense from a perspective of balance. But it also presents military leaders with a dilemma. They are responsible for fighting the war of ideas in an age where they must quickly come up with proactive messages and reactive responses. This demand calls for a decentralized approach to strategic communication and information engagement.[33] The means to achieve that speed, the Internet, is indispensable to the conduct of daily business, yet it is under continuous surveillance and attack, causing some leaders to place it under centralized control. This issue tips toward either point based on the level of risk a commander is willing to take in the information environment, and the organizational culture of the military regarding the value of competing in that environment.

Addressing the Dilemma: Managing Risk, Achieving Balance

A command approach focusing on a "defense in depth" to secure the NIPRnet and controlling outside access to and use of the Internet, while understandable from a threat analysis approach, flies in the face of the tenets of good strategy and military planning:

> Strategic thinking [is] a sophisticated intellectual process seeking to create a synthesis of consensus, efforts, and circumstances to influence the overall environment favorably while managing the risks involved in pursuing opportunities or reacting to threats.[34]

Therefore, a strategy regarding use of the Internet to influence the information environment requires managing the risk of attack while pursuing the opportunities to compete. The previously cited definition of cyberpower as the "ability to create advantages and influence events" in cyberspace appears to provide a proactive, offensive-minded focus on cyber-related activities. *The National Strategy for Combating Terrorism* notes the opportunity the Internet offers to discredit adversary propaganda. The June 2008 *National Defense Strategy* discusses the requirement to mitigate risk—but in terms of the ability to exploit opportunity.[35] Still, it remains to be seen whether commanders will take a risk-averse approach to the new DOD policy by establishing centralized control emphasizing defense of the network.[36]

Military operations rely on centralized planning and decentralized execution with a synchronized overarching plan that subordinate organizations adhere to in their subordinate plans to achieve desired ends. Decentralized execution fosters agility, speed, and responsiveness in a fluid and constantly changing environment. Therefore, if information is a key component of current and future military operating environments, it follows that a centralized plan with decentralized execution would hold in cyberspace.

Again, however, some commands' emphasis regarding the Internet may restrict decentralized execution, hampering the ability to be proactive, agile, and responsive in prosecuting the war of ideas.

The question is how to exploit emerging cyber capabilities to influence perceptions, attitudes, and behaviors while managing the risk of surveillance and attack of the Internet. It is important to consider the various reasons given to limit access to new media means since they inform the logic of those commands prone to restricting access: to promote work productivity, support bandwidth requirements, maintain operations security, and prevent intrusion and compromise. These examples are clearly covered in new DOD policy. Still, this expansion is necessary to provide a reasoned argument in favor of the balanced approach that policy directs.

Productivity. One argument for using NIPRnet content filters to preclude access to video upload sites (e.g. YouTube), blogs, and social networking sites is the assumption that Soldiers will access them for personal use during duty hours, thus adversely affecting work productivity. Certainly, that potential exists. However, the responsibility to manage this issue is leader business, pure and simple, and should be handled on a by-exception basis. Content filters established at any level of command usurp the responsibilities of leaders in subordinate organizations.

Bandwidth requirements. Another argument for restricting access to video uplink sites is the requirement to manage bandwidth requirements. Bandwidth is the "capacity to move information."[37] It is a low-density, high-demand item in providing command and control computer capabilities to the military. However, again, leaders decide how to distribute any valuable, limited resource to support mission requirements and accomplish the military mission.[38]

Operations security. Operations security "selects and executes measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation."[39] Some leaders worry that participation by military members in blogging, social networking, and uploading to video sites can potentially reveal military vulnerabilities. This risk applies to both the NIPRnet and the Internet where military members may conduct new media engagement from home. It is certainly a risk borne out by several significant violations in recent years. However, OPSEC is, and always has been, a commander's program. Commanders control the OPSEC environment through training, education, and punitive measures for deliberate violations. Content filters and command policies established at high levels to prevent OPSEC violations are restrictions that detract from the subordinate commander's ability to lead and achieve military objectives by exploiting the capabilities of the network.

Intrusions and the threat of compromise of the network itself are, on the other hand, valid and important concerns. DOD systems, as previously noted, are under continuous attack by nation-states, nonstate actors, criminals, and hackers. Consequently, the department was right to establish a system that reduces gateways to the Internet and allows judicious and continuous monitoring, to prevent the downloading of software that might harbor malicious code with devastating consequences to the network, and to continue to evaluate ways to mitigate such risk. Adversaries and criminals alike continuously adapt to updates and other defensive measures.

Managing risk while providing the opportunity to engage effectively and exploit the opportunities the Internet provides requires a rebalancing of command philosophy. Leaders and commanders have the authority and resources to conduct rapidly proactive and responsive strategic communication. Productivity, bandwidth, and OPSEC issues are clearly leader business, and leaders should monitor subordinates and hold them accountable for violations of their guidance. This decentralized approach assumes risk. Commanders and leaders must take steps to mitigate this risk but in a balanced fashion.

Lieutenant General William Caldwell says (interestingly using a blog as his medium of choice) we should encourage Soldiers to tell their stories, empower them by underwriting honest mistakes, educate them on potential strategic implications

Managing risk … to engage effectively… requires a rebalancing of command philosophy.

of engagement, and equip them to engage the new media.[40] While Caldwell specifically refers to physical equipment, one could reasonably argue that equally, if not more importantly, is equipping Soldiers with the appropriate command guidance that freely allows engagement by new media means while prescribing the limits of that interaction. The new DOD policy, as it trickles down to subordinate commands, should allow free engagement provided commanders are open to the opportunities and aware of the threats.

Conclusion

In August 2008, Russia apparently again conducted cyber attacks, but this time in a coordinated and synchronized kinetic and nonkinetic campaign against Georgia.[41] It is entirely probable that this may become the norm in future warfare between and among nation-states that can conduct such complex excursions. The case of Hezbollah in the 2006 conflict with Israel also suggests the future strategic use of the Internet and new media to strike at domestic and international audiences.

The information environment has three dimensions: the physical dimension, the "means" by which one sends a message; the informational dimension, or content of the message; and the cognitive dimension, or the impact of the message on the perceptions, attitudes, and behaviors of target audiences.[42] It's safe to say that future war will increasingly include conflict in cyberspace in all three dimensions.

Exploiting opportunity while managing risk is the strategic imperative. A good military plan, whether on land, sea, or air, will "protect the force" while attacking the enemy. Civilian leaders and military commanders weigh risk, emplace policies, and act to mitigate risk, but they also focus on achieving policy and military objectives. In cyberspace, this means both protecting the Internet and using it to engage.

Considering second- and third-order effects when making decisions is also important. Given the constant threat of a successful cyber attack against U.S. government systems, leaders might default to the no risk or low risk option of strengthening the virtual walls around the NIPRnet to impervious levels. Moreover, to prevent the potential violation of operations security, they may establish restrictive policies on the use of the Internet. However, the second-order effect of doing all this is to significantly reduce the ability of leaders and commanders to engage in the information environment using new media.

Currently, U.S. government and military strategies "talk the talk" in this regard with encouraging evidence toward "walking the walk." Senior leader guidance to engage audiences using new media trumpets the beginnings of overcoming a long-standing cultural bias against using the Internet for important information engagements. New DOD policy offers the opportunity to achieve the balance necessary to both exploit and protect the Internet. Leaders and commanders are responsible for fighting wars. A more restrictive NIPRnet will not resolve this dilemma and, in fact, can have significant adverse second-order effects. It's time to break down some of the risk-averse culture to allow "maneuver" to occur so that leaders at all levels can do their job. ***MR***

NOTES

1. The U.S. Army published its doctrinal manual on counterinsurgency, Field Manual 3-24 (Washington, DC: U.S. Government Printing Office [GPO], December, 2006). The foreword notes that the Army had not reviewed its counterinsurgency doctrine in over 20 years and cites the ongoing operations in Iraq and Afghanistan as the impetus for the effort.

2. Huba Wass de Czege, "Lessons from the Past: Making the Army's Doctrine 'Right Enough' Today," *Landpower Essay, Institute of Land Warfare*, no. 06-2 (September 2006): 4, 5.

3. Robert H. Scales, *Certain Victory: The U.S. Army in the Gulf War* (Washington, DC: Brassey's, 1997), 106-107.

4. Demitry Sevastopulo and Richard McGregor, "Chinese Military Hacked into Pentagon," *Financial Times*, 4 September 2007.

5. Anne Applebaum, "e-Stonia Under Attack," 22 May 2007, <www.slate.com/id/2166716/> (18 August 2008).

6. Kevin Peraino, "Winning Hearts and Minds," *Newsweek International*, 2 October 2006.

7. Chairman of the Joint Chiefs of Staff, "DOD Dictionary of Military Terms," as amended through 30 October 2009.

8. Daniel Kuehl, "From Cyberspace to Cyberpower, Defining the Problem," in *Cyberpower and National Security* (Washington: National Defense University Press, 2009), 38.

9. *National Strategy for Combating Terrorism* (Washington, DC: GPO, September, 2006), 4, 17.

10. Kevin J. Cogan and Raymond G. Delucio, "Network Centric Warfare Case Study, vol. II" (Carlisle Barracks, PA: U.S. Army War College, 2006), 4.

11. Ronald Deibert, presentation, U.S. Army War College, Carlisle Barracks, PA, 10 January 2008. Deibert cites <www.internetworldstats.com> as a source document for these statistics. Updated as of 30 March 2009.

12. William R. Levesque, "Blogs are CENTCOM's New Target," *Saint Petersburg Times*, 12 February 2007.

13. Carmen L. Gleason, "Coalition Servicemembers Reach out to America via YouTube," *American Forces Press Service*, 14 March 2007.

14. Sevastopulo and McGregor, "Chinese Military Hacked into Pentagon."

15. Timothy L. Thomas, *DragonBytes: Chinese Information War Theory and Practice* (Foreign Military Studies Office: Fort Leavenworth, KS, 2004), 136.

16. Joseph Glebocki, "DOD Computer Network Operations: Time to Hit the Send Button" (Carlisle Barracks, PA: U.S. Department of the Army, 15 March 2008), 4.

17. Stephen Blank, "Web War I: Is Europe's First Information War a New Kind of War," *Comparative Strategy* 27, no. 3 (May 2008): 240.

18. Applebaum, "e-Stonia Under Attack."

19. Blank, 230.

20. Stephanie Condon, "DHS Stays Mum on New 'Cyber Security' Center," 31 July 2008, <http://news.cnet.com/8301-13578_3-10004266-38.htm> (4 August 2008).

21. Chairman of the Joint Chiefs of Staff, Joint Publication 3-13, *Information Operations*" (Washington, DC: GPO, September, 2006,13 February 2006), II-5, II-6.

22. The author attended a conference on cyberpower sponsored by the Center for Technology and National Security Policy at the National Defense University in Washington, D.C. in April 2008. The referenced comments reflect panelists' presentations. The conference was held under Chatham House rules allowing free and open dialog while ensuring the anonymity of speakers.

23. Tony Capaccio, "Cyber Attacks from China Show Computers Insecure, Pentagon Says," 6 August 2008, <www.bloomberg.com/apps/news?pid=newsarchive&sid=aGqtPqPlSCt8> (18 August 2008).

24. U.S. Department of Defense, *QDR Execution Roadmap for Strategic Communication* (Washington DC: U.S. Department of Defense, September 2006), 3.

25. Office of the Deputy Assistant Secretary of Defense for Joint Communication (DASD(JC)), presentation, June 2008. DASD(JC) is responsible for the Quadrennial Defense Review Strategic Communication Roadmap and Strategic Communication education and training within the Department of Defense.

26. LTG William Caldwell, "Changing the Organizational Culture," 30 January 2008, <http://smallwarsjournal.com/blog/2008/01/changing-the-organizational-cu-1/> (18 August 2008).

27. Elizabeth Robbins, "Muddy Boots IO: The Rise of Soldier Blogs," *Military Review*, no. 5 (September-October 2007), 116.

28. Ernesto Londono, "Silent Posting," *Washington Post*, 24 July 2008.

29. The author has been present at numerous presentations at the U.S. Army War College where senior leaders (general officers and senior Army civilians) have advocated aggressive use of new media means to get out the positive messages about service members. An April 2008 memo co-signed by the Chief of Staff of the Army and Secretary of the Army urged a significant effort to tell the story of support of Army families using "new media such as blogs as effective means for communicating" the message.

30. Commander, Combined Arms Center, LTG William Caldwell, "Request for Exception to Policy for Publishing to a Publically Accessible Website," memorandum for Commander, U.S. Army Training and Doctrine Command et al., 27 March 2008.

31. U.S. Deputy Secretary of Defense Gordon England, "Policy for Department of Defense (DOD) Interactive Internet Activities," memorandum for Secretaries of the Military Departments et al., 8 June 2007.

32. U.S. Deputy Secretary of Defense William Lynn, "Responsible and Effective Use of Internet-based Capabilities," memorandum for Secretaries of the Military Departments et al., 25 February 2010.

33. The Army Field Manual on operations (February 2008), devotes a chapter to the topic of information as a warfighting capability. It stresses the need for "information engagement" at the individual Soldier level. It further discusses the requirement to overcome a risk-averse culture in order to effectively engage. See chap. 7.

34. Harry R. Yarger, *Strategic Theory for the 21st Century: The Little Book on Big Strategy* (Carlisle Barracks, PA: Strategic Studies Institute, 2006), 36.

35. U.S. Department of Defense, *National Defense Strategy* (Washington, DC: U.S. Department of Defense, June 2008). See the "Strategic Framework."

36. Recently the author was unable to access Facebook in a recent visit to the Combined Arms Center at Fort Leavenworth, KS, where he intended to show its military enabling effects to military students.

37. Tim Wu, "OPEC 2.0," *New York Times*, 30 July 2008.

38. John B. Tisserand, "Network Centric Warfare Case Study, Volume I" (Carlisle Barracks, PA: U.S. Army War College, 2006), 53.

39. Chairman of the Joint Chiefs of Staff, "DOD Dictionary of Military Terms," as amended through 31 October 2009.

40. Caldwell, "Changing the Organizational Culture."

41. John Markoff, "Before the Gunfire, Cyberattacks," *New York Times*, 13 August 2008.

42. Joint Publication 3-13, *Information Operations*, I-1-I-2.